Applications of tripled chaotic maps in cryptography

Sohrab Behnia[a]*, Afshin Akhshani[a], Amir Akhavan[b], Hadi Mahmodi[a]

[a] *Department of Physics, IAU, Urmia, Iran*

[b] *Department of Engineering, IAU, Urmia, Iran*

Abstract

Security of information has become a major issue during the last decades. New algorithms based on chaotic maps were suggested for protection of different types of multimedia data, especially digital images and videos in this period. However, many of them fundamentally were flawed by a lack of robustness and security. For getting higher security and higher complexity, in the current paper, we introduce a new kind of symmetric key block cipher algorithm that is based on *tripled chaotic maps*. In this algorithm, the utilization of two coupling parameters, as well as the increased complexity of the cryptosystem, make a contribution to the development of cryptosystem with higher security. In order to increase the security of the proposed algorithm, the size of key space and the computational complexity of the coupling parameters should be increased as well. Both the theoretical and experimental results state that the proposed algorithm has many capabilities such as acceptable speed and complexity in the algorithm due to the existence of two coupling parameter and high security. Note that the ciphertext has a flat distribution and has the same size as the plaintext. Therefore, it is suitable for practical use in secure communications.

1 Introduction

Chaos theory is a blanketing theory that covers most aspects of science, hence, it shows up everywhere in the world today: mathematics, physics, biology, finance, computer and even music. As we know, chaotic systems have many interesting features, such as the sensitivity to the initial condition and control parameter, ergodicity and mixing property [1, 2, 3, 4], which can be connected with some cryptographic properties of good ciphers, such as confusion/diffusion, balance and

*E-mail: s.behnia@iaurmia.ac.ir

avalanche property [5, 6]. These properties make the chaotic systems a worthy choice for constructing the cryptosystems. Compared with traditional cryptosystems [7], the ones based on chaos are more suitable for large-scale data encryption such as images, videos or audio data. Furthermore, chaos-based algorithms have shown their good performance. Thus, it is a natural idea to use chaos as a new source to construct new encryption systems. Cryptography has become one of the fields of modern science since the celebrated Shannon's work [8]. In general, the algorithms used for cryptographic applications are classified into two, namely, public key (Asymmetric methods) cryptography and secret key (Symmetric methods) cryptography. According to the structure of the symmetric algorithm, ciphers can be divided into two categories, namely, block ciphers [9] and stream ciphers [10]. The chaotic cryptography technique which we are going to use in this paper belongs to a symmetric block cipher. There exist two main approaches of designing chaos-based cryptosystems: analog and digital. The first one is generally based on the concept of chaotic synchronization, initiated by the work of Pecora and Carroll [11], and the concerned chaotic systems are implemented in analog form. The second one is independent of chaos synchronization and the chaotic systems are completely implemented in digital computers [4, 12]. The present paper mainly focuses on the digital chaotic ciphers.

In the digital world, which is currently evolving and changing at such a rapid pace, the security of digital information has become increasingly more important. This is due to the communications of digital products over network occurring more and more frequently. So that in recent years, many different chaotic cryptosystems in digital domain have been proposed [13, 14, 15, 16, 17, 18, 19]. Certainly, a main issue in all encryption techniques is their security. However, the recent development of chaotic cryptosystem is rather disappointing. On the other hand, various cryptanalysis have exposed some inherent drawbacks of chaotic cryptosystems [20, 21, 22, 23]. Some of these shortcomings are overviewed in [24, 25, 26].

For enhancing the security of discrete chaotic cryptosystem in this paper for the first time, we introduce the concept of using hierarchy of tripled chaotic maps with an invariant measure in cryptography. Six points make this new cryptosystem distinctive and advantageous compared to the other schemes.

- A very large number of fully developed chaotic maps defined in two intervals $x \in [0, 1]$ and $x \in [0, \infty)$.
- Bifurcation without any period doubling; bifurcation from a stable single periodic state to chaotic ones without having usual period doubling or period-n-tupling scenario.
- The existence of the two coupling parameters. One advantage of using two coupling parameters is for computational complexity goal. Another advantage is the usage of coupling parameters in the structure of the cryptosystem for diffusion. These parameters can be used as secret keys as well.

- High complexity due to high dimensionality and chaoticity.
- Large key space; It is obvious that the attack complexity is determined by the size of the key space and the complexity of the verification of each key.
- The flexibility of attributing different values to the control parameters.

Besides the above advantages, the encryption speed is also acceptable and the ciphertext has the same size as the plaintext. In fact, the results presented in this paper totalize our earlier work [27].
This paper has been organized as follows: Section 2 describes the construction and the main features of the tripled chaotic maps. Current encryption schemes are introduced briefly in section 3. The experimental results are shown in section 4. Section 5 demonstrates the security of the proposed scheme. Finally, conclusions are drawn in Section 6.

2 Tripled Chaotic Maps

We first review the one parameter families of trigonometric chaotic maps which are used to construct the tripled chaotic maps. One-parameter families of chaotic maps of the interval [0, 1] with an invariant measure can be defined as the ratio of polynomials of degree N [28]:

$$\Phi_N^{(1,2)}(x,\alpha) = \frac{\alpha^2 F}{1+(\alpha^2-1)F}, \tag{1}$$

Where **F** substitute with chebyshev polynomial of type one $T_N(x)$ for $\Phi_N^{(1)}(x,\alpha)$ and chebyshev polynomial of type two $U_N(x)$ for $\Phi_N^{(2)}(x,\alpha)$[29]. As an example we give below some of these maps:

$$\phi_2^{(1)} = \frac{\alpha^2(2x-1)^2}{4x(1-x)+\alpha^2(2x-1)^2}, \quad \phi_2^{(2)} = \frac{4\alpha^2 x(1-x)}{1+4(\alpha^2-1)x(1-x)},$$

The map $\Phi_2^{(2)}(x,\alpha)$ is reduced to logistic one with $\alpha = 1$. One can show that these maps have two interesting properties. It is shown that these maps have interesting property, that is, for even values of N the $\Phi^{(1)}(\alpha,x)(\Phi^{(2)}(\alpha,x))$ maps have only a fixed point attractor $x = 1(x = 0)$ provided that their parameter belongs to interval $(N,\infty)((0,\frac{1}{N}))$ while, at $\alpha \geq N$ $(\alpha \geq \frac{1}{N})$ they bifurcate to chaotic regime without having any period doubling or period-n-tupling scenario and remain chaotic for all $\alpha \in (0,N)$ $(\alpha \in (\frac{1}{N},\infty))$ but for odd values of N, these maps have only fixed point attractor at $x = 0$ for $\alpha \in (\frac{1}{N},N)$, again they bifurcate to a chaotic regime at $\alpha \geq \frac{1}{N}$, and remain chaotic for $\alpha \in (0,\frac{1}{N})$, finally they bifurcate at $\alpha = N$ to have $x = 1$ as fixed point attractor for all $\alpha \in (\frac{1}{N},\infty)$. We used their conjugate

or isomorphic maps. Conjugacy means that the invertible map $h(x) = \frac{1-x}{x}$, maps $I = [0, 1]$ into $[0, \infty)$ and transform maps $\Phi_N(x, \alpha)$ into $\tilde{\Phi}_N(x, \alpha)$ defined as:

$$\tilde{\Phi}_N^{(1)}(x, \alpha) = \frac{1}{\alpha^2} \tan^2(N \arctan \sqrt{x}), \tag{2}$$

$$\tilde{\Phi}_N^{(2)}(x, \alpha) = \frac{1}{\alpha^2} \cot^2(N \arctan \frac{1}{\sqrt{x}}), \tag{3}$$

Using the hierarchy of families of one-parameter chaotic maps (1), we can generate new hierarchy of tripled maps with an invariant measure. Hence, by introducing a new parameter ϵ as a coupling parameter we form coupling among the above mentioned maps, where they can be coupled through β and α functions defined as:

$$\beta(x(n)) = (\sqrt{\beta_0} + \epsilon x(n))^2, \tag{4}$$

$$\alpha_N(x(n)) = \frac{B_N(\frac{1}{\beta(x(n))})}{A_N(\frac{1}{\beta(x(n))})} \sqrt{\frac{\beta(x(n+1))}{\beta(x(n))}}, \tag{5}$$

with $B_N(x)$ and $A_N(x)$ defined as:

$$A_N(x) = \sum_{k=0}^{[\frac{N}{2}]} C_{2k}^N x^k, \quad B_N(x) = \sum_{k=0}^{[\frac{N-1}{2}]} C_{2k+1}^N x^k, \tag{6}$$

Now, the hierarchy of the tripled chaotic maps can be defined as:

$$\Phi_{N_1,N_2,N_3} = \begin{cases} x_1(n+1) = \Phi_{N_1}(x_1(n), \alpha_1(x_2(n), x_3(n))), \\ x_2(n+1) = \Phi_{N_2}(x_2, \alpha_2(x_3(n))), \\ x_3(n+1) = \Phi_{N_3}(x_3(n), \alpha_3), \end{cases} \tag{7}$$

Also, their conjugate or isomorphic maps by considering the map $h(x) = \frac{1-x}{x}$ are defined as follows:

$$\tilde{\Phi}_{N_1,N_2,N_3} = \begin{cases} \tilde{x}_1(n+1) = \frac{1}{\alpha_1^2(x_2(n),x_3(n))} \tan^2(N_1 \arctan \sqrt{x_1(n)}), \\ \tilde{x}_2(n+1) = \frac{1}{\alpha_2^2(x_3(n))} \tan^2(N_2 \arctan \sqrt{x_2(n)}), \\ \tilde{x}_3(n+1) = \frac{1}{\alpha_3^2} \tan^2(N_3 \arctan \sqrt{x_3(n)}), \end{cases} \tag{8}$$

As we know, each dynamical system has specific characteristics. In fact, the differences between discrete dynamical systems arise from these properties. Due to this fact, in this paper, tripled chaotic maps are constructed for the first time. So, it is necessary to describe them through the paper. Specially, the most important characteristics such as invariant measure and Lyapunov characteristic exponents have been discussed.

Furthermore, many properties of the chaotic systems have their corresponding counterparts in traditional cryptosystems, such as: ergodicity and confusion, sensitivity to initial conditions/control parameter and diffusion [30]. For tripled chaotic maps, we have tried to describe ergodicity from the invariant measure point of view.

2.1 Invariant measure

Dynamical systems, even apparently simple dynamical systems which are described by maps of an interval can display a rich variety of different asymptotic behavior. On measure theoretical level these type of behavior are described by SRB [31, 32] or invariant measure describing statistically stationary states of the system. The probability measure μ on $[0,1]$ is called an SRB or invariant measure of the map $y = \Phi_N(x,\alpha)$ given in Eqs. (2)and(3), if it is $\Phi_N(x,\alpha)$-invariant and absolutely continuous with respect to Lebesgue measure. For deterministic system such as $\Phi_N(x,\alpha)$-map, the $\Phi_N(x,\alpha)$-invariance means that, its invariant measure $\mu(x)$ fulfills the following formal FP integral equation:

$$\mu(y) = \int_0^1 \delta(y - \Phi_N(x,\alpha))\mu(x)dx,$$

This is equivalent to:

$$\mu(y) = \sum_{x\in\Phi_N^{-1}(y,\alpha)} \mu(x)\frac{dx}{dy}, \tag{9}$$

defining the action of standard FP operator for the map $\Phi_N(x,\alpha)$ over a function as:

$$P_{\Phi_N} f(y) = \sum_{x\in\Phi_N^{-1}(y,\alpha)} f(x)\frac{dx}{dy}, \tag{10}$$

We see that, the invariant measure $\mu(x)$ is actually the eigenstate of the FP operator P_{Φ_N} corresponding to largest eigenvalue 1. As it is proved, in our previous work, the invariant measure $\mu_{\Phi_N(x,\alpha)}(x,\beta_0)$ has the following form (for more detail see [28]):

$$\mu(x) = \frac{1}{\pi}\frac{\sqrt{\beta_0}}{\sqrt{x(1-x)}(\beta_0 + (1-\beta_0)x)}, \tag{11}$$

with $\beta_0 > 0$, is the invariant measure of maps Eqs. (2)and(3) provided that, we choose the parameter α, in the following form :

$$\alpha = \frac{\sum_{k=0}^{[\frac{(N-1)}{2}]} C_{2k+1}^N \beta_0^{-k}}{\sum_{k=0}^{[\frac{N}{2}]} C_{2k}^N \beta_0^{-k}}, \tag{12}$$

in $\Phi_N^{(1,2)}(x,\alpha)$ maps for odd values of N and

$$\alpha = \frac{\beta_0 \sum_{k=0}^{[\frac{(N)}{2}]} C_{2k}^N \beta_0^{-k}}{\sum_{k=0}^{[\frac{(N-1)}{2}]} C_{2k+1}^N \beta_0^{-k}}, \tag{13}$$

in $\Phi_N^{(2)}(x,\alpha)$ maps for even values of N. Similarly the probability measure μ for tripled chaotic maps Φ_{N_1,N_2,N_3} given in Eq. (7) fulfills the following formal FP integral equation, where for simplicity we consider their conjugate maps Eq. (8):

$$\mu(y_1,y_2,y_3)=\int dx_1\int dx_2\int dx_3\delta(y_1-\tilde{x}_1(x_1,x_2,x_3))\delta(y_2-\tilde{x}_2(x_1,x_2))$$

$$\times\delta(y_3-\tilde{x}_3(x_3))\mu(x_1,x_2,x_3),$$

which is equivalent to:

$$\mu(y_1,y_2,y_3)=\sum_{x\varepsilon\tilde{\Phi}^{-1}_{N_1,N_2,N_3}}\mid J(x_1,x_2,x_2),\mid\mu(x_1,x_2,x_3), \tag{14}$$

where $J(x_1,x_2,x_2)$ is the Jacobian of the transformation $\tilde{\Phi}_{N_1,N_2,N_3}$ which is equal to:

$$J(x_1,x_2,x_2)=\frac{\partial(\tilde{x}_1,\tilde{x}_2,\tilde{x}_3)}{\partial(y_1,y_2,y_3)},$$

again defining the action of standard FP operator for the map Φ_{N_1,N_2,N_3} over a function as:

$$P_{\tilde{\Phi}_{N_1,N_2,N_3}}f(y)=\sum_{x\in\tilde{\Phi}^{-1}_{N_1,N_2,N_3}}f(x)J(x_1,x_2,x_3), \tag{15}$$

We see that, the invariant measure $\mu(x_1,x_2,x_3)$ is also the eigenstate of the FP operator $P_{\tilde{\Phi}_{N_1,N_2,N_3}}$ corresponding to largest eigenvalue 1. As it is proved in Appendix A the invariant measure $\mu_{\tilde{\Phi}_{N_1,N_2,N_3}}(x_1,x_2,x_3)$ has the following form:

$$\mu=\frac{1}{\pi}\frac{\sqrt{\beta_0}}{\sqrt{x_3(1-x_3)}(\beta_0+(1-\beta_0)x_3)}\times\frac{1}{\pi}\frac{\sqrt{\beta(x_3)}}{\sqrt{x_2(1-x_2)}(\beta(x_3)+(1-\beta(x_3))x_2)}$$

$$\times\frac{1}{\pi}\frac{\sqrt{\beta(x_2,x_3)}}{\sqrt{x_1(1-x_1)}(\beta(x_2,x_3)+(1-\beta(x_2,x_3))x_1)}, \tag{16}$$

with $\beta>0$ and given in Eq. (4) and Eqs. (12)and(13).

2.2 Lyapunov characteristic exponent

The method of measuring disorder in a dynamical system, is based on the concept of Lyapunov Characteristic Exponents (LCE). For one-dimensional maps, LCE characterizes the local stretching, determined by the mapping $d\phi_n(x,\alpha)$, weighted

by the probability of encountering that amount of stretching, that is probability of a trajectory visiting a particular location **x**. Here we compute LCE for tripled chaotic maps as the characteristic exponent of the rate of average magnification of the neighborhood of an arbitrary point $\vec{r}_0 = (x_{1_0}, x_{2_0}, x_{3_0})$ and it is denoted by $\lambda(\overrightarrow{r_0})$, which can be written as [32]:

$$\lambda(\vec{r}_0) = \lim_{n\to\infty} \sum_{k=0}^{n-1} \ln | \frac{\partial(\overbrace{(\Phi \circ \Phi \circ .... \circ \Phi)}^{k}_1, \overbrace{(\Phi \circ \Phi \circ .... \circ \Phi)}^{k}_2, \overbrace{\Phi \circ \Phi \circ .... \circ \Phi)}^{k}_3)}{\partial(x_{1_0}, x_{2_0}, x_{3_0})} |$$

$$\lambda(\vec{r}_0) = \lim_{n\to\infty} \sum_{k=0}^{n-1} \ln | \frac{\partial x_{N_1}(x_k, \alpha_1)}{\partial x_{1_0}} . \frac{\partial x_{N_2}(x_k, \alpha_2)}{\partial x_{2_0}} . \frac{\partial x_{N_3}(x_k, \alpha_3)}{\partial x_{3_0}} | \tag{17}$$

where $x_k = \overbrace{\Phi \circ \Phi \circ .... \circ \Phi}^{k}$. A positive LCE implies that two nearby trajectories exponentially diverge (at least locally). Negative LCE indicates contraction along certain directions, and zero LCE indicates that along the relevant directions there is neither expansion nor contraction. The equality of KS-entropy and sum of all positive LCE;

$$h_{KS} = \sum_{\lambda_l > 0} \lambda_l,$$

indicates that in chaotic region, this map is ergodic as Birkhoff ergodic theorem predicts [33].

3 The Encryption and Decryption Procedures

In this section the framework of our proposed algorithm is described. The proposed cryptosystem is a symmetric key block cipher algorithm based on tripled chaotic maps. Note that the Lyapunov characteristic exponent is positive, that is, the tripled maps are chaotic in nature. According to [34], a possible way to describe the key space might be in terms of positive Lyapunov exponents. For this reason we have selected all of the control parameters in the chaotic region. A block diagram illustrating the complete procedure of the proposed scheme is depicted in Fig. 1. First, plaintext is divided into blocks of the same sizes (8-bit)and the blocks are transformed into a matrix $M_{1\times n}$, .In matrix M each element of the matrix represents one block, and n is the total number of the blocks. The tripled maps are iterated using coupling parameters, control parameters and initial conditions. In the iteration process first 100 iterations are ignored to avoid transient effects. The matrix element $M_{1\times i}$ in each round is encrypted as below:

$$C_{1\times i} = M_{1\times i} \text{ XOR } (\tilde{x}_f \bmod 256),$$

where $\tilde{x}_f$ is a long integer generated using $\tilde{x}_1$, $\tilde{x}_2$ and $\tilde{x}_3$ and some simple mathematical operators. In each round coupling parameters and $\tilde{x}_f$ are regenerated using $C_{1\times i-1}$, $\tilde{x}_1$, $\tilde{x}_2$ and some simple mathematical operators. While the process reaches the last element, the elements of matrix $C_{1\times n}$ are reversed and $M_{1\times n}$ is set equal to new matrix $C_{1\times n}$. Then again the process starts from the beginning. In fact, the plaintext is encrypted once from the beginning to the end and once from end to the beginning. Thus, a very small change in the plaintext will result in a completely different ciphertext. In this cryptosystem, the process of decryption is completely similar to the encryption process. For decryption process, the only difference is that the following new relation is used instead of aforesaid relation.

$$M_{1\times i}=C_{1\times i} \text{ XOR } (\tilde{x}_f \bmod 256),$$

As an example, the following maps are selected from the chaotic maps(Eq.8) to be used in encryption/decryption process.

$$\tilde{\Phi}_{2,2,14}(\tilde{x}_1,\tilde{x}_2,\tilde{x}_3)=\begin{cases}\tilde{x}_1(n+1)=\frac{1}{\alpha_1^2(x_2(n),x_3(n))}\tan^2(2\arctan\sqrt{x_1(n)}),\\ \tilde{x}_2(n+1)=\frac{1}{\alpha_2^2(x_3(n))}\tan^2(2\arctan\sqrt{x_2(n)}),\\ \tilde{x}_3(n+1)=\frac{1}{\alpha_3^2}\tan^2(14\arctan\sqrt{x_3(n)}),\end{cases} \tag{18}$$

with

$$\alpha_2(x_3(n))=\frac{2\beta(x_3(n))}{1+\beta(x_3(n))}\sqrt{\frac{\beta(x_3(n+1))}{\beta(x_3(n))}},\quad \beta(x_3(n))=(\sqrt{\frac{\alpha_2}{2-\alpha_2}}+\epsilon x_3(n))^2,$$

$$\alpha_1(x_2(n),x_3(n))=\frac{2\beta(x_2(n),x_3(n))}{1+\beta(x_2(n),x_3(n))}\sqrt{\frac{\beta(x_2(n+1),x_3(n+1)))}{\beta(x_2(n),x_3(n))}},$$

$$\beta(x_2(n),x_3(n))=(\sqrt{\frac{\alpha_1}{2-\alpha_1}}+\epsilon' x_2(n))^2,$$

4 Experimental Results

In this section, we provide some experimental results to illustrate the performance of the proposed chaotic cryptosystem. In order to test the efficiency of the proposed chaotic cryptographic scheme, we used the scheme in the following files.

File 1: Text (.txt) file of size 30 720 bytes;

File 2: Word document (.doc) file of size 210 944 bytes;

File 3: Executable (.exe) file of size 487 000 bytes;

File 4: Audio (.mp3) file of size 980 304 bytes;

File 5: Image (.bmp) file of size 65 536 bytes;

File 6: Video clip (.avi) file of size 1 087 430 bytes.

The encryption and decryption time for all of source files mentioned above are listed in Table 1.
The length of the ciphertext is the same as thought the plain text. This features is another most important features of our introduced cryptosystem(See the last column of Table 1). Note that, the previous cryptosystems like Baptista-type chaotic cryptosystems [35, 36, 37] had almost double-sized ciphertext.
In order to compare the performance evaluation of the proposed method with the previous work [27], from the security point of view, we focus on the application of this method in image encryption. We assume that source image is 65 536 bytes. Fig. 2(a) shows the experimental results with Bird BMP image. Fig. 2(b) is its encrypted image with the encryption keys mentioned below. According to Eq. (18), encryption keys are chosen as follows: $\tilde{x}_3$=66, $\tilde{x}_2$=444, $\tilde{x}_1$=445 as initial conditions and ϵ=0.2, ϵ'=0.5 as a coupling parameters and finally α_3=1.5, α_2=0.455, α_1=0.2 as control parameters. We have implemented the proposed algorithm using C++ programming language and observed the simulation results on a Pentium-IV 2.4 GHz Celeron D with 256MB RAM and 80 Gb hard-disk capacities. It seems that, our encryption time is acceptable compared to that of encryption times mentioned in [38, 39, 40].

5 Security Analysis

When a new cryptosystem is proposed, it should always be accompanied by some security analysis. A good encryption procedure should be robust against all kinds of cryptanalytic, statistical and brute-force attacks. Here, some security analysis has been performed on the proposed scheme, including some important ones like key space analysis, statistical analysis, etc. The security analysis demonstrated the high security of the new scheme, as demonstrated in the following.

5.1 Key space analysis

A fundamental aspect of every cryptosystem is the key. An algorithm is as secure as its key. No matter how strong and well designed the algorithm might be, if the key is poorly chosen or the key space is small enough, the cryptosystem will be broken. The size of the key space is the number of encryption/decryption key pairs that are available in the cipher system. Apparently, the attack complexity is determined by the size of the key space and the complexity of verifying each key. From the cryptographical point of view, the size of the key space should not be smaller than 2^{100} to provide a high level of security [6, 41]. If the precision 10^{-16}, the key space

size for initial conditions, control parameters and coupling parameters is over than 2^{400}. It seems that the key space is large enough to resist all kinds of brute-force attacks.

In addition, one attempt to describe the dynamics of the current system is by providing bifurcation diagram and determining interesting properties of it. In any case, the designer of any chaotic cryptosystem should conduct a study of chaotic regions of the parameter space from which valid keys, i.e., parameter values leading to chaotic behavior, can be chosen. When many parameters are used simultaneously as part of the key, the mutual interdependence complicates the task of deciding which intervals are suitable. Only keys chosen from the black region of bifurcation diagram are suitable enough [42, 43]. In this cryptosystem, the interval of the initial condition is $[0, \infty)$. From the bifurcation diagram it is clear that the maps are chaotic for any x with respect to control parameters in chaotic region. In Fig. 3, we have depicted a portion of the bifurcation diagram of $\tilde{\Phi}_N^{(1)}(x, \alpha)$ while N=2. As we can see, within the black region, there isn't any periodic windows, so the entire black region is suitable for robust keys.

5.2 Statistical analysis

In his masterpiece, Shannon [8] said, "It is possible to solve many kinds of ciphers by statistical analysis," and therefore, he suggested two methods of diffusion and confusion for the purpose of frustrating the powerful statistical analysis. This is shown by a test on the histograms of the ciphered images, on the correlations of adjacent pixels in the ciphered image and on the distribution of the ciphertext.

1.Histograms of ciphered images. By taking a (256×256) sized Bird image as a plaintext, the histograms of the plaintext and its corresponding ciphertext are as follows. It is clear that the encrypted image is confused and cannot be understood. Moreover, the histogram of the encrypted image is uniformly distributed, which makes statistical attacks very difficult (See Figs. 4(a) and 4(b)).

2. Correlation of two adjacent pixels. Statistical analysis has been performed on the proposed image encryption algorithm by a test on the correlation of adjacent pixels in the plain-image and ciphered image. To analyze the correlations of the adjacent pixels, we can use Eq. (19) to calculate the correlation coefficients in horizontal, vertical and diagonal [14, 44].

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))(y_i - E(y)), \quad r_{xy} = \frac{cov(x, y)}{\sqrt{D(x)}\sqrt{D(y)}}, \tag{19}$$

where

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i, \qquad D(x) = \frac{1}{N}\sum_{i=1}^{N}(x_i - E(x))^2.$$

$E(x)$ is the estimation of mathematical expectations of x, $D(x)$ is the estimation of variance of x and $cov(x, y)$ is the estimation of covariance between x and y. where

x and y are grey-scale values of two adjacent pixels in the image. We randomly choose 1000 image pixels in the plain image and the ciphered image respectively to calculate the correlation coefficients of the adjacent pixels in horizontal. The correlation coefficients of the adjacent pixels in vertical and in diagonal are calculated and listed in Table 2 and the distribution is shown in Figs. 5(a) and 5(b). It demonstrates that the encryption algorithm has covered up all the characters of the plain image and shows good performance of balanced 0-1 ratio.
In addition to analysis mentioned above, we have also analyzed the distribution of the ciphertext. Therefore, we have recorded the number of occurrences of each ciphertext block for one of the six source files. A typical distribution of the ciphertext is shown in Figs. 6(a) and 6(b), which shows that the distribution is very flat due to the masking operation. Totally, statistical analysis has been performed on the proposed encryption algorithm, demonstrating its superior confusion and diffusion properties which strongly resist statistical attacks.

5.3 Information entropy

Information theory is a mathematical theory of data communication and storage founded in 1949 by Claude E. Shannon. To calculate the entropy *H(s)* of a source s, we have:

$$H(s) = \sum_{i=0}^{2N-1} P(s_i) \log_2 \frac{1}{P(s_i)}, \tag{20}$$

where $P(s_i)$ represents the probability of symbol s_i. Actually, given that a real information source seldom transmits random messages, in general, the entropy value of the source is smaller than the ideal one. However, when these messages are encrypted, their entropy should ideally be 8. If the output of such a cipher emits symbols with an entropy of less than 8, then there exists a predictability which threatens its security. We have calculated the information entropy for encrypted image Fig. 2(b):

$$H(s) = \sum_{i=0}^{255} P(s_i) \log_2 \frac{1}{P(s_i)} = 7.9978$$

The obtained value is very close to the theoretical value 8. Apparently, comparing it with the other existing algorithms, such as [15], the proposed algorithm is much more closer to the ideal situation. This means that information leakage in the encryption process is negligible, and so the encryption system is secure upon the entropy attack.

5.4 Differential attack

As we know, if one minor change in the plain-image can cause a significant change in the ciphered-image, with respect to both diffusion and confusion, then this "dif-

ferential attack" may become inefficient. To test the influence of one-pixel change on the whole image, encrypted by the proposed chaos-based algorithm, two common measures may be used: Number of Pixels Change Rate (NPCR) and Unified Average Changing Intensity (UACI) [45, 46]. We take two encrypted images, C_1 and C_2, whose corresponding original images have only one-pixel difference. We label the grey scale values of the pixels at grid (i,j) of C_1 and C_2 by $C_1(i,j)$ and $C_2(i,j)$, and C_1 and C_2 have the same size. Then, $D(i,j)$ is determined by $C_1(i,j)$ and $C_2(i,j)$, that is, if $C_1(i,j) = C_2(i,j)$, then, $D(i,j) = 1$; otherwise,$D(i,j) = 0$. NPCR and UACI are defined by the following formulas:

$$NPCR = \frac{\sum_{i,j} D(i,j)}{W \times H} \times 100\%$$

$$UACI = \frac{1}{W \times H}\left[\sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255}\right] \times 100\%$$

Where, W and H are the width and length of the image. We obtained NPCR=0.34 % and UACI=0.33 %. With regard to obtained results, apparently, the proposed algorithm has a good ability to resist differential attack.

6 Conclusion

In this paper, after introducing hierarchy of tripled chaotic maps with invariant measure, we investigated their potential for exploitation as a cryptosystem. These maps have interesting features such as invariant measure, ergodicity and variable control parameters. In addition to some features aforesaid, the most important advantage of these maps is the existence of the two coupling parameters. It seems that the excellent efficiency of the new cryptosystem is derived from this property. In this scheme, its structural parameters and initial values can all be used as encryption key in chaotic cryptosystem. Therefore, the size of key space is very large. Statistical analysis performed on the proposed encryption algorithm, demonstrates its superior confusion and diffusion properties which strongly resist statistical attacks. Experimental results illustrate that the distribution of the ciphertext is very flat and the entropy, is almost equal to the ideal value. Moreover, the encryption time is acceptable while the size of ciphertext is the same as that of the plaintext. The present paper's goal is to construct a practical and fully secure cryptosystem. Our experiments indicate that this goal is almost achieved. Based on all analysis and experimental results, the conclusion is that, from a cryptographical point of view, the proposed scheme is a good candidates for practical applications in information security fields.

Acknowledgment

The authors would like to express their heartfelt gratitude to Mr. A. Bonyadi for the nice editing of their paper - this has certainly improved its readability.

Appendix A: Derivation of the invariant measure In order to prove that measure Eq. (16) satisfies Eq. (14), it is rather convenient to consider the conjugate map. By inverting the conjugate map Eq. (8) we get:

$$\begin{cases} x_{k3} = \tilde{\Phi}^{-1}_{N_3}(x_3, \alpha_3)), \\ x_{k2,k3} = \tilde{\Phi}^{-1}_{N_2}(x_2, \alpha_2(x_{k3})), \\ x_{k1,k2,k3} = \tilde{\Phi}^{-1}_{N_1}(x_1, \alpha_1(x_{k2,k3}, x_{k3})), \end{cases} \tag{.1}$$

Now, considering the following anzatz for invariant measure

$$\mu(x_1, x_2, x_3) = \frac{1}{\pi} \frac{\gamma(x_2, x_3)}{(1 + \beta(x_2, x_3)x_1)\sqrt{x_1}}, \tag{.2}$$

where

$$\int \frac{\gamma(x_2, x_3)}{\sqrt{\beta(x_2, x_3)}} dx_2 dx_3 = 1.$$

The probability measure μ for coupled chaotic maps Φ_{N_1,N_2,N_3} given in Eq. (7) fulfills the following formal FP integral equation (Eq. 14):

$$\mu(x_1, x_2, x_3) = \sum_{k1,k2,k3} \mid \frac{\partial x_{k1,k2,k3}}{\partial x_1} \frac{\partial x_{k2,k3}}{\partial x_2} \frac{\partial x_{k3}}{\partial x_3} \mid \mu(x_{k1,k2,k3}, x_{k2,k3}, x_{k3}) \tag{.3}$$

by taking the derivative of last term of Eq. (A.1) with respect to x_1, we have:

$$\frac{\partial x_{k1,k2,k3}}{\partial x_1} = \frac{\alpha_1(x_{k2,k3}, x_{k3})}{N_1} \frac{\sqrt{x_{k1,k2,k3}}(1 + x_{k1,k2,k3})}{\sqrt{x_1}(1 + \alpha_1^2(x_{k2,k3}, x_{k3})x_1)} \tag{.4}$$

from Eq. (A.2) it follows that:

$$\frac{\gamma(x_2, x_3)}{(1 + \beta(x_2, x_3)x_1)\sqrt{x_1}} = \sum_{k1,k2,k3} \frac{\alpha_1}{N_1} \frac{(1 + x_{k1,k2,k3})}{\sqrt{x_1}(1 + \alpha_1^2(x_{k2,k3}, x_{k3})x_1)}$$

$$\times \frac{\gamma(x_{k2,k3}, x_{k3})}{1 + \beta(x_{k2,k3}, x_{k3})x_{k1,k2,k3}} \tag{.5}$$

we readily see that

$$\sum_{k3} \frac{\alpha_1}{N_1} \frac{(1 + x_{k1,k2,k3})}{(1 + \beta(x_{k1,k2,k3}))} = \frac{\alpha_1 A_{N_1}(\beta^{-1}(x_{k2,k3}, x_{k3}))}{B_{N_1}(\beta^{-1}(x_{k2,k3}, x_{k3}))}$$

$$\times \frac{(1 + \alpha_1^2(x_{k2,k3}, x_{k3}))x_1)}{1 + \beta(x_{k2,k3}, x_{k3})(\frac{A_{N_1}(\beta^{-1})\alpha_3}{B_{N_1}(\beta^{-1})})^2 x_1} \tag{.6}$$

Eq. (A.3) reduce to:

$$\frac{\gamma(x_2, x_3)}{(1 + \beta(x_2, x_3)x_1)} = \sum_{k1,k2,k3} \frac{\partial x_{k2,k3}}{\partial x_2} \frac{\partial x_{k3}}{\partial x_3}$$

$$\times \frac{\alpha_1(x_{k2,k3},x_{k3})A_{N_1}(\beta^{-1}(x_{k2,k3},x_{k3}))}{B_{N_1}(\beta^{-1}(x_{k2,k3},x_{k3}))}\frac{1}{1+\beta(x_{k1})(\frac{A_{N_1}(\beta^{-1})\alpha_1}{B_{N_1}(\beta^{-1})})^2x_1}, \tag{.7}$$

which is possible if $\beta(x_2,x_3)$ and $\beta(x_{k2,k3},x_{k3})$ are related as:

$$\left(\frac{\alpha_1 A_{N_1}(\beta^{-1}(x_{k2,k3},x_{k3}))}{B_{N_1}(\beta^{-1}(x_{k2,k3},x_{k3}))}\right)^2\beta(x_{k2,k3},x_{k3})=\beta(x_2,x_3) \tag{.8}$$

therefore, the relation Eq. (A.7) reduces to

$$\frac{\gamma(x_2,x_3)}{\sqrt{\beta(x_2,x_3)}}=\sum_{k2,k3}\frac{\partial x_{k2,k3}}{\partial x_2}\frac{\partial x_{k3}}{\partial x_3}\frac{\gamma(x_{k2,k3},x_{k3})}{\sqrt{\beta(x_{k2,k3},x_{k3})x_{k3}}}=\mu(x_2,x_3) \tag{.9}$$

By considering

$$\frac{\gamma(x_2,x_3)}{\sqrt{\beta(x_2,x_3)}}=\frac{1}{\pi}\frac{\gamma(x_3)}{\sqrt{x_2}(1+\beta(x_3)x_2)} \tag{.10}$$

where

$$\int\frac{\gamma(x_3)}{\sqrt{\beta(x_3)}}dx_3=1$$

which is possible if $\beta(x_3)$ and $\beta(x_{k3})$ are related as:

$$\left(\frac{\alpha_2(x_3)A_{N_2}(\beta^{-1}(x_{k3}))}{B_{N_2}(\beta^{-1}(x_{k3}))}\right)^2\beta(x_{k3})=\beta(x_3) \tag{.11}$$

or Eq. (A.9) can be written as:

$$\frac{\gamma(x_3)}{\sqrt{\beta(x_3)}}=\sum_{k3}\frac{\partial x_{k3}}{\partial x_3}\frac{\gamma(x_{k3})}{\sqrt{\beta(x_{k3})}}=\frac{1}{\pi}\frac{\beta}{\sqrt{x_3}(1+\beta x_3)}$$

hence it is proportional to its invariant measure.

References

[1] Hao B-L. Starting with Parabolas: an introduction to chaotic dynamics. Shanghai Scientific and Technological Education Publishing House. Shanghai China; 1993.

[2] Lasota A, Mackey MC. Chaos, fractals and noise-stochastic aspects of dynamics. 2nd edn., New York, Springer; 1994.

[3] Blank M. Discreteness and continuity in problems of chaotic dynamics. Monograph. Amer Math Soc; 1997.

[4] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurcat Chaos 1998;8(6):1259-84.

[5] Brown R, Chua LO. Clarifying chaos: examples and counterexamples. Int J Bifurcat Chaos 1996;6(2):219-49.

[6] Schneier B. Applied cryptography- protocols, algorithms, and source code in c. 2nd ed. New York, John Wiley & Sons; 1996.

[7] Buchmann JA. Introduction to cryptography. Springer, New York; 2001.

[8] Shannon CE. Communication theory of secrecy systems, Bell Syst. Tech J. 1949;28:656-715.

[9] Tsueike M, Ueta T, Nishio Y. An application of two-dimensional chaos cryptosystem. Tech Rep of IEICE NLP 1996; 96-19.

[10] Lee PH, Pei SC, Chen YY. Generating chaotic stream ciphers using chaotic systems. Chinese J Phys 2003;41:559-81.

[11] Pecora LM, Carroll TL. Synchronization in chaotic systems. Phys Rev Lett 1990;64:821-24.

[12] Baptista MS. Cryptography with chaos. Phys Lett A 1998;240:50-4.

[13] Wei J, Liao X, Wong KW, Xiang T. A new chaotic cryptosystem. Chaos, Solitons & Fractals 2006;30:1143-52.

[14] Chen G, Mao YB, Chui CK. A symmetric image encryption scheme based on 3d chaotic cat maps. Chaos Solitons & Fractals 2004;21:749-61.

[15] Xiang T, Liao X, Tang G, Chen Y, Wong KW. A novel block cryptosystem based on iterating a chaotic map. Phys Lett A 2006;349:109-15.

[16] Xiao D, Liao X, Wong K. An eciententire chaos-based scheme for deniable authentication. Chaos, Solitons & Fractals 2005;23:1327-31.

[17] Tang G, Liao X, Chen Y. A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons & Fractals 2005;23:413-19.

[18] Zhang L, Liao X, Wang X. An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals 2005;24:759-65.

[19] Behnia S, Akhshani A, Ahadpour S, Mahmodi H, Akhavan A. A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps. Phys Lett A [Article in press] DOI:10.1016/j.physleta.2007.01.081.

[20] Dachselt F, Schwarz W. Chaos and cryptography, IEEE Trans Circ Syst 2001;48(12):1498-1509.

[21] Kocarev L. Chaos-based cryptography: a brief overview, IEEE Circ Syst 2001;1:6-21.

[22] Zhou C, Lai CH. Extracting messages masked by chaotic signals of time-delay systems. Phys Rev E 1999;60:320-23.

[23] Alvarez G. Security problems with a chaos-based deniable authentication scheme. Chaos, Solitons & Fractals 2005;26:7-11.

[24] Li S, Mou X, Cai Y, Ji Z, Zhang J. On the security of a chaotic encryption scheme: problems with computerized chaos in finite computing precision, Comput Phys Commun 2003;153(1):52-58.

[25] Li S, Mou X, Yang BL, Ji Z, Zhang J. Problems with a probabilistic encryption scheme based on chaotic systems. Int J Bifurcat Chaos 2003;13(10):3063-77.

[26] Jakimoski G, Kocarev L. Analysis of some recently proposed chaos-based encryption algorithms. Phys Lett A 2001; 291(6):381-84.

[27] Behnia S, Akhshani A, Mahmodi H, Akhavan A. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals [Article in press] DOI:10.1016/j.chaos,(2006.05.011).

[28] Jafarizadeh MA, Behnia S, Khorram S, Naghshara H. Hierarchy of chaotic maps with an invariant measure. J Stat Phys 2001;104:1013-28.

[29] Wang ZX, Guo DR. Special functions. World Scientific Publishing; 1989.

[30] Alvarez G, Hernandez L, Munoz J, Montoya F, Li S. Security analysis of communication system based on the synchronization of different order chaotic systems. Phys Lett A 2005;345:245-50.

[31] Cornfeld IP, Fomin SV, Sinai YG. Ergodic theory. Berlin, Springer; 1982.

[32] Dorfman JR. An introduction to chaos in nonequilibrium statistical mechanics. Cambridge: Cambridge University Press; 1999.

[33] Keller G. Equlibrium states in ergodic theory. Cambridge: Cambridge University Press; 1998.

[34] Alligood K, Sauer T, Yorke J. Chaos- An introduction to dynamical systems. Springer; 1997.

[35] Alvarez G, Montoya F, Romera M, Pastor G. Key stream cryptanalysis of a chaotic cryptographic method. Comput Phys Commun 2004;156(2):205-7.

[36] Wong KW. A fast chaotic cryptographic scheme with dynamic look-up table. Phys Lett A 2002; 298(4):238-242.

[37] Wong W-K, Lee L-P, Wong K-W. A modified chaotic cryptographic method. Comput Phys Commun 2001;138(3):234-36.

[38] Wong K-W, Ho S-W, Yung C-K. A chaotic cryptography scheme for generating short ciphertext. Phys Lett A 2003;310:67-73.

[39] Wong K-W. A combined chaotic cryptographic and hashing scheme. Phys Lett A 2003;307:292-98.

[40] Wong K-W, Man K-P, Li S, Liao X. A more secure chaotic cryptographic scheme based on dynamic look-up table. Circuits, Systems and Signal Processing 2005;24(5):571-84.

[41] Stinson DR. Cryptography: theory and practice. CRC Press; 1995.

[42] Alvarez G, Li S. Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcat Chaos 2006;16(8):2129-51.

[43] Alvarez G, Montoya F, Romera M, Pastor G. Breaking parameter modulated chaotic secure communication system. Chaos, Solitons & Fractals 2004;21:783-87.

[44] Bluman AG. Elementary statistics. 3rd ed. New York, McGraw-Hill; 1998.

[45] Mao YB, Chen G, Lian SG. A novel fast image encryption scheme based on 3D chaotic baker maps. Int J Bifurcat Chaos 2004;14(10):3613-24.

[46] Chen G, Ueta T. Yet another chaotic attractor. Int J Bifurcat Chaos 1999;9(7):1465-66.

Table 1: Performance of the proposed chaotic cryptographic on the six files, encryption/decryption time

	Plaintext file size (bytes)	Encryption time (in seconds) min.-max. (mean)	Ciphertext file size (bytes)
File 1 (.txt)	30 720	0.14-0.15 (0.145)	30 720
File 2 (.doc)	210 944	1.005-1.007 (1.006)	210 944
File 3 (.exe)	487 000	2.5-2.56 (2.53)	487 000
File 4 (.mp3)	980 304	0.44-0.47 (0.455)	980 304
File 5 (.bmp)	65 536	0.33-0.36 (0.345)	65 536
File 6 (.avi)	1 087 430	5.61-5.67 (5.64)	1 087 430

Table 2: Correlation coefficients of two adjacent pixels in two images

	Plain image	Ciphered image
Horizontal	0.9902	0.000029549
Vertical	0.9815	0.00045066
Diagonal	0.9721	0.000013

Figures Caption:

Fig. 1: Block Diagram.

Fig. 2: (a) Plain image, (b) Ciphered image.

Fig. 3: Bifurcation diagram of $\tilde{\Phi}_N^{(1)}(x, \alpha)$ while N=2.

Fig. 4: (a) Histogram of plain image, (b) Histogram of ciphered image.

Fig. 5: (a) Correlation analysis of plain image, (b) Correlation analysis of ciphered image.

Fig. 6: (a) Distribution of the plaintext, (b) Distribution of the ciphertext.

This figure "Fig1.jpg" is available in "jpg" format from:

http://arXiv.org/ps/0705.2633v1

This figure "Fig2.jpg" is available in "jpg" format from:

http://arXiv.org/ps/0705.2633v1

This figure "Fig2b.jpg" is available in "jpg" format from:

http://arXiv.org/ps/0705.2633v1

This figure "Fig3.jpg" is available in "jpg" format from:

http://arXiv.org/ps/0705.2633v1


This figure "Fig4a.jpg" is available in "jpg" format from:
http://arXiv.org/ps/0705.2633v1

This figure "Fig4b.jpg" is available in "jpg" format from:

http://arXiv.org/ps/0705.2633v1


This figure "Fig5a.jpg" is available in "jpg" format from:
http://arXiv.org/ps/0705.2633v1

This figure "Fig5b.jpg" is available in "jpg" format from:

http://arXiv.org/ps/0705.2633v1


This figure "Fig6a.jpg" is available in "jpg" format from:
http://arXiv.org/ps/0705.2633v1

This figure "Fig6b.jpg" is available in "jpg" format from:

http://arXiv.org/ps/0705.2633v1